CÓDIGO LIBRE

MENTES LIBRES

SOFTWARE LIBRE PARA UNA SOCIEDAD LIBRE

open source

CYPHERPUNK ES LIBERTAD

SOBERANÍA, RESISTENCIA, Y AUTODEFENSA ELECTRÓNICA

EN TELÉFONOS MÓVILES: PARTE 3

PRIVACIDAD
SOBERANÍA
RESISTENCIA
AUTONOMÍA
LIBERTAD

ESTA GUÍA CUBRE:

CONTRASEÑAS SEGURAS
Entropía, gestión y autenticación de dos factores.

AMENAZAS EN REDES WIFI
Rastreo, ataques y protección en redes inalámbricas.

PRIVACIDAD EN ANDROID
Permisos, datos, telemetría y hardening del sistema.

COMUNICACIONES SEGURAS
Cifrado de extremo a extremo, mensajería y llamadas seguras.

SOFTWARE LIBRE Y HERRAMIENTAS
Apps libres, código abierto y control total de tu dispositivo.

INFORMACIÓN ES PODER. PRIVACIDAD ES LIBERTAD. RESISTENCIA ES FUTURO.

PROTÉGETE • INFÓRMATE • ORGANÍZATE • RESISTE

1110 0101

Sección I: Configuraciones de Seguridad y Privacidad

1.1 Contraseñas Seguras - Análisis Avanzado

Las contraseñas son la primera línea de defensa para proteger dispositivos y cuentas. Una contraseña robusta maximiza la **entropía**, que es la medida de impredecibilidad: mientras más entropía, más difícil es adivinarla mediante fuerza bruta.

- **Longitud y entropía:** Se recomienda una longitud mínima de 10 caracteres. La entropía se aproxima con la fórmula *log2(n^L)*, donde *n* es el número de símbolos disponibles y *L* la longitud de la contraseña. Por ejemplo, con 94 símbolos posibles (letras mayúsculas, minúsculas, dígitos y caracteres especiales), un password aleatorio de 10 caracteres tiene alrededor de 66 bits de entropía. Cada carácter adicional duplica la dificultad para el atacante. En la práctica, una clave de 12 o 16 caracteres aleatorios ofrece una resistencia exponencialmente mayor a ataques de fuerza bruta, dificultando que un atacante logre descifrarla incluso con hardware especializado. No obstante, debido a la limitación humana para memorizar cadenas muy largas, se debe equilibrar la longitud con técnicas de gestión seguras.
- **Complejidad y variedad:** Mezclar tipos de caracteres incrementa la entropía. Limitarse a minúsculas (26 opciones) es mucho más débil que incluir mayúsculas y símbolos. Agregar números y símbolos puede aumentar el alfabeto efectivo a más de 90 caracteres. También se recomienda usar espacios o crear frases clave largas (*passphrases*). Por ejemplo, la frase **«La casa azul!»** (13 caracteres, incluyendo espacio y símbolo) contiene mucha más entropía que 13 caracteres aleatorios por su longitud y mezcla de categorías. Incluir mayúsculas intercaladas, dígitos en lugar de letras o símbolos poco comunes dificulta enormemente los ataques basados en diccionario o patrones previsibles.
- **No repetición y rotación:** Nunca se debe reutilizar la misma contraseña en distintos servicios. Si una cuenta se ve comprometida, las demás permanecerán seguras con contraseñas distintas. Del mismo modo, cambiar contraseñas periódicamente puede prevenir accesos prolongados tras una filtración. Sin embargo, cambios muy frecuentes (cada mes, por ejemplo) suelen conducir a pequeñas variaciones obvias (añadir un número secuencial o fecha), lo que puede facilitar la tarea al atacante. Es más seguro rotar contraseñas únicamente ante sospechas de brecha de seguridad conocida. Mantener un registro seguro de versiones (por

ejemplo, dentro de un gestor cifrado) ayuda a evitar repetir contraseñas antiguas o variantes triviales.

- **Gestión de contraseñas:** Dada la complejidad necesaria, es recomendable usar gestores de contraseñas confiables. Estas herramientas generan y almacenan contraseñas cifradas, liberando al usuario de la tarea de memorizarlas. Emplear un gestor con una **contraseña maestra** fuerte y única asegura que solo el usuario autorizado pueda acceder al resto de claves. Otra estrategia eficaz es usar *passphrases*: combinaciones de palabras aleatorias o frases largas que son fáciles de recordar pero muy difíciles de adivinar debido a su longitud. Por ejemplo, elegir al azar cuatro palabras (como «roca lámpara río tren») puede dar una contraseña de 20 o más caracteres con enorme entropía. Además, activar la autenticación de dos factores (2FA) añade una capa extra: incluso si se filtra la contraseña, el atacante necesitaría un segundo factor (código de app, llave física o SMS) para completar el acceso.

1.2 Amenazas en Redes WiFi - Análisis Técnico

Las redes inalámbricas desprotegidas son terreno fértil para intrusos. Durante el reconocimiento WiFi, los dispositivos emiten peticiones para detectar redes conocidas y su propia dirección MAC, lo que puede ser monitoreado. Los atacantes profesionales utilizan herramientas de escaneo (como **wardriving** con antenas especiales) para mapear redes cercanas e identificar dispositivos objetivo por su huella y dirección MAC.

- **Técnicas de rastreo:** Cada dispositivo tiene una dirección MAC única. Aunque los sistemas operativos modernos ofrecen aleatorización de MAC, no siempre se activa y muchos dispositivos aún revelan su dirección real al buscar redes. Esto permite a un atacante rastrear la presencia de un usuario en diferentes ubicaciones siguiendo la misma MAC. Además, las señales periódicas (*beacons*) de routers o puntos de acceso pueden ser recolectadas para mejorar el seguimiento. En algunos entornos se utilizan WiFi *sniffers* o sensores pasivos que detectan la actividad de los dispositivos, revelando incluso cuándo un teléfono entra o sale de un área. Estas técnicas permiten perfilar movimientos y hábitos de los usuarios sin que ellos lo perciban.
- **Vulnerabilidades de protocolos WiFi:** Las versiones antiguas de WiFi presentan fallas graves. WEP está obsoleto: con pocos paquetes capturados se descifra en minutos con herramientas conocidas. WPA y WPA2 son más fuertes, pero no infalibles. Por ejemplo, el ataque **KRACK** explota

debilidades en el protocolo de negociación de claves de WPA2 para descifrar tráfico cifrado. Además, mecanismos como WPS (Wi-Fi Protected Setup) pueden ser inseguros: un PIN de emparejamiento de solo 8 dígitos facilita ataques de fuerza bruta en el PIN. También existen vulnerabilidades en routers con firmware sin actualizar, que podrían permitir la ejecución de comandos remotos o la alteración de la configuración de seguridad. Por ello, siempre hay que mantener actualizado el firmware del punto de acceso y usar los protocolos más seguros disponibles (WPA2/WPA3 con cifrado AES).

- **Ataques Man-in-the-Middle (MITM):** En redes públicas abiertas, un atacante puede interponerse entre el usuario y el punto de acceso. Mediante *ARP spoofing*, el intruso se hace pasar por el router legítimo, redirigiendo el tráfico a través de su dispositivo. Asimismo, crear un punto WiFi falso ("**evil twin**") con nombre similar al de una red confiable puede engañar a usuarios desprevenidos, quienes sin saberlo se conectan a él. Cuando el tráfico pasa por el atacante, éste puede monitorear o modificar datos (credenciales, sitios visitados, mensajes, etc.), especialmente si no se usan protocolos cifrados. Por ejemplo, sesiones HTTP sin HTTPS pueden ser leídas o alteradas. Incluso con cifrado WPA, si el atacante conoce la contraseña (o utiliza claves por defecto) puede descifrar el tráfico. En resumen, cualquier conexión a WiFi desconocido o público es susceptible de interceptación.
- **Mitigación:** Para protegerse, conectarse solo a redes WiFi seguras (WPA2/WPA3 con contraseñas robustas). Cambiar periódicamente la contraseña del WiFi propio y no compartirla públicamente ayuda a evitar intrusiones internas. Además, es fundamental usar VPN o aplicaciones que cifren su propio tráfico (HTTPS, TLS) para proteger la información aunque la red externa falle. Se recomienda desactivar la conexión automática a redes conocidas y ocultar el SSID de la red propia para que no se divulgue. También conviene deshabilitar el escaneo pasivo del dispositivo (que envía sondas a redes guardadas), de modo que el móvil no revele cuáles redes busca. Por último, siempre verificar los certificados de los sitios web (asegurarse de navegar mediante HTTPS válido) evita caer en redes falsas que pretendan ser legítimas.

1.3 Actualizaciones Constantes - Análisis de Seguridad

Mantener el sistema operativo y las aplicaciones al día es fundamental para cerrar vulnerabilidades conocidas. Cada parche de seguridad corrige fallos que

de otro modo podrían ser aprovechados por atacantes; ignorarlos deja abiertos agujeros listos para explotación.

- **Prevención de bugs y vulnerabilidades:** Todo software tiene errores inevitables. Cuando se descubren fallos (por ejemplo, desbordamientos de búfer, escalada de privilegios o ejecución remota), los fabricantes publican actualizaciones que los corrigen. Aplicar estos parches regularmente cierra esos canales de ataque. Por ejemplo, un agujero en el sistema de archivos que permitía acceso root fue neutralizado mediante un parche oficial. No actualizar el sistema equivale a dejar una puerta trasera abierta. Al instalar las últimas versiones se reducen errores conocidos, se refuerzan los controles internos y se bloquea el aprovechamiento de exploits públicos.
- **Ciberseguridad y parches:** El ciclo de seguridad implica reportar vulnerabilidades, analizarlas y distribuir soluciones. Organizaciones como CERT emiten avisos (CVE) sobre exploits conocidos. Los usuarios deben habilitar actualizaciones automáticas o revisar periódicamente nuevas versiones del sistema y de las apps instaladas. Actualizar no solo refuerza la seguridad; a menudo incluye mejoras de estabilidad y rendimiento. Un teléfono vulnerable, sin los parches adecuados, puede ser blanco de ataques de malware masivo que explotan fallos viejos: basta visitar un sitio malicioso o recibir un archivo comprometido para quedar infectado. Las actualizaciones evitan precisamente eso.
- **Ciclo de vida de actualizaciones:** Cada plataforma móvil (Android, iOS, etc.) ofrece soporte por un tiempo limitado. Una vez que el sistema alcanza su “fin de vida”, deja de recibir parches oficiales. Usar un dispositivo fuera de soporte implica que nuevas vulnerabilidades jamás tendrán corrección. Por eso, es prudente migrar a versiones o dispositivos más actuales antes de que caduque el soporte. Mientras aún reciben atención, instalar la última versión disponible reduce drásticamente la superficie de ataque. Conocer las fechas de fin de soporte (por ejemplo, cuando el fabricante deja de actualizar un modelo) permite planificar la renovación y no exponerse a riesgos prolongados.
- **Riesgos de no actualizar:** Un teléfono desactualizado es presa fácil. Los atacantes escanean versiones antiguas en busca de vulnerabilidades públicas. Por ejemplo, un exploit en el navegador web puede permitir la instalación de malware simplemente visitando una página comprometida. Cada día que un parche de seguridad se omite, aumenta la ventana de exposición: es como dejar abierta la misma vulnerabilidad que ya fue

documentada. Además, muchos virus o troyanos avanzados detectan automáticamente la versión del sistema y usan fallos conocidos para infiltrarse. En definitiva, la falta de actualizaciones pone en peligro tanto la integridad del dispositivo como la confidencialidad de los datos personales.

Sección II: Amenazas y Protecciones Avanzadas

2.1 Amenazas en Redes Bluetooth - Análisis de Riesgos

Bluetooth es práctico para conexiones de corto alcance, pero también puede actuar como una puerta trasera si permanece activo innecesariamente. Aunque su rango es menor que el WiFi, un atacante puede aproximarse y escanear dispositivos emparejados y descubiertos, aprovechando debilidades del protocolo.

- **Vectores pasivos:** Un atacante puede usar un sniffer Bluetooth para detectar dispositivos cercanos, incluso si no están emparejados. Cada dispositivo Bluetooth tiene una dirección única (MAC), la cual se transmite durante la búsqueda. Dejar el Bluetooth encendido expone el dispositivo: quien escanee repetidamente puede inferir su presencia y movilidad. Además, algunos auriculares o altavoces Bluetooth anuncian nombres de dispositivo o identificadores que, combinados, ayudan a rastrear al usuario a lo largo del tiempo. Estas señales revelan la presencia del móvil en proximidad sin que el usuario lo note.
- **Protocolos y vulnerabilidades:** Históricamente, Bluetooth ha tenido vulnerabilidades graves. El ataque **BlueBorne** (2017) permitía ejecución de código remoto sin necesidad de emparejamiento, aprovechando fallos en la pila Bluetooth. Versiones antiguas usaban códigos PIN cortos (como “0000”) para emparejar, lo cual podía ser interceptado. Las versiones previas a Bluetooth 4.2 no cifraban adecuadamente la información de emparejamiento. Si el firmware del dispositivo no está actualizado, puede quedar expuesto a exploits conocidos. Cada salto de versión (Bluetooth 4.x, 5.x, etc.) ha mejorado la seguridad, pero muchos aparatos antiguos siguen siendo vulnerables.
- **Técnicas de explotación:** Ejemplos de ataque incluyen *bluesnarfing* (robo de datos personales vía Bluetooth), *bluebugging* (control remoto del teléfono para enviar mensajes o realizar llamadas) y *bluejacking* (envío de mensajes anónimos a dispositivos). Aunque el *bluejacking* suele ser solo una molestia (envío de SMS o mensajes emergentes), demuestra que el canal puede ser usado sin autorización. También existen ataques de fuerza

bruta contra el PIN de emparejamiento o secuestro de sesiones mal implementadas. Un atacante avanzado podría, tras lograr emparejarse con un dispositivo vulnerable, emitir comandos como si fuera el usuario, leer mensajes o incluso activar micrófono.

- **Defensa:** Para protegerse, la recomendación principal es dejar el Bluetooth apagado cuando no sea necesario. Si se necesita, conviene configurarlo en modo “no visible” u “oculto” para evitar ser detectado durante los escaneos pasivos. Emparejar los dispositivos siempre bajo las opciones más seguras (por ejemplo, escaneando códigos QR o usando NFC), y actualizar el firmware del teléfono y accesorios con regularidad. Además, revisar periódicamente los dispositivos conectados –y eliminar los desconocidos– evita conexiones indeseadas. Rechazar solicitudes de emparejamiento sospechosas y cambiar el nombre del dispositivo a algo irreconocible (en lugar del modelo exacto) ayudan a reducir la huella de Bluetooth visible.

2.2 Servicios VPN para Protección de Privacidad

Una VPN (Virtual Private Network) cifra el tráfico entre el móvil y sus servidores, resguardando la navegación. Varias VPN destacadas ofrecen características de privacidad avanzadas:

- **Mullvad (Suecia):** Conocido por su estricta política *no-logs*. No requiere correo electrónico para abrir cuenta; se crea una ID alfanumérica. Acepta pagos anónimos (criptomonedas, efectivo). Emplea OpenVPN y WireGuard con cifrado AES-256 y SHA-512. Mullvad publica auditorías externas que confirman su ausencia de registros. También ofrece multihop (conexión doble) y tiene servidores que no registran marcas de tiempo ni direcciones IP. Es ideal para usuarios que buscan anonimato puro sin dejar huella.
- **ProtonVPN (Suiza):** Desarrollado por ProtonMail, con fuerte enfoque en privacidad. Opera bajo jurisdicción suiza. Ofrece OpenVPN, IKEv2/IPSec y WireGuard. Destaca su función *Secure Core*, que enruta el tráfico a través de múltiples servidores (p. ej. en Suiza e Islandia) antes de salir a Internet, protegiendo contra vigilancia estatal. ProtonVPN no guarda registros de usuarios y permite conexiones a la red Tor. Su infraestructura de alta calidad lo hace robusto frente a censura y confiable para uso diario.
- **iVPN (Países Bajos):** VPN enfocada en privacidad, auditada por terceros. Soporta OpenVPN y WireGuard; todos sus servidores son de propiedad propia (para evitar riesgo de terceros). No guarda registros de conexión ni direcciones IP. Admite *multihop* (rutas dobles entre servidores). Acepta pagos en criptomonedas y su cliente es sencillo. Su enfoque minimalista y

transparencia técnica son valorados por usuarios que desean configuración robusta sin complicaciones.

- **AirVPN (Italia):** Creado por activistas, sin registros y con alto nivel técnico. Ofrece OpenVPN personalizado (TLS-auth, cifrado 4096-bit RSA para control) y permite conexiones TCP o UDP. Da opción de multihop y está orientado al usuario avanzado. Su cliente ("Eddie") es de código abierto y brinda controles detallados (p. ej., ajuste de puerto, proxy interno). AirVPN no limita la velocidad ni protocolos; es una buena opción para compartición P2P o para quienes desean un control granular sobre la conexión cifrada.
- **NymVPN:** Vinculado al proyecto Nym de anonimato, NymVPN combina VPN con redes de mezcla (mixnets). Encapsula las conexiones en túneles adicionales de cifrado más allá del VPN normal, ocultando patrones de tráfico. Aún emergente, implementa túneles a través de la red descentralizada de Nym, lo que aporta anonimato extra. Admite cifrado estándar (por ejemplo, AES-256) y tiene enfoque innovador en ocultamiento de metadatos.
- **Cryptostorm:** Opera bajo la filosofía *StormVPN*. Usa múltiples capas de cifrado (encadenamiento de OpenVPN) y no registra actividad. Ofrece integración con Tor (permitiendo enrutar conexiones a través de la red Tor por defecto) y acepta pagos en diversas criptomonedas. Emplea un sistema de "clave" anual en lugar de usuario/contraseña. Su base legal en Suiza y políticas independientes lo hacen resistente a presiones legales, lo que refuerza la confianza en su privacidad.
- **VPN.cd:** Servicio con sede en Estados Unidos o Nepal (según la jurisdicción de sus servidores), enfocado en privacidad. Utiliza cifrado fuerte (OpenVPN con AES-256, IKEv2) y no mantiene registros de tráfico ni IP. Tiene servidores en múltiples países y permite amplio control técnico (elección de puertos, túneles divididos, etc.). Su punto fuerte es la simplicidad combinada con privacidad: la política abierta de no-logs brinda confidencialidad a sus usuarios sin demasiadas restricciones de uso.

Protocolos y cifrado: La mayoría de las VPN mencionadas utiliza protocolos auditados como OpenVPN o WireGuard. Ambos soportan cifrado simétrico AES-256 (garantizando confidencialidad) y autenticación SHA-2/3 para integridad. Algunos servicios también ofrecen IKEv2/IPSec (útil en móviles por reconexión rápida) o tecnologías ofuscadas para evadir censura (como Obfsproxy). Es importante, al configurar el cliente VPN en el teléfono, elegir un protocolo moderno y cifrado fuerte. Por ejemplo, WireGuard suele ofrecer mejor

rendimiento y seguridad comparado con PPTP o L2TP (obsoletos). En general, OpenVPN UDP con AES-256/GCM es un estándar confiable para dispositivos móviles.

Políticas de no registro (no-logs): Es crítico que el proveedor no guarde registros de actividad, sitios visitados o direcciones IP. Todas las VPN listadas han demostrado (mediante auditorías o reputación) mantener esa promesa. Mullvad, ProtonVPN e iVPN tienen claras políticas *no-logs*. AirVPN y Cryptostorm también son conocidos por su transparencia. Se recomienda revisar las condiciones de cada servicio: si el proveedor publica informes de auditoría externa y aclara que no almacena logs, ofrece mayor garantía. Incluso con cifrado fuerte, un VPN que registre datos perdería anonimato real en caso de solicitudes legales o brechas.

Selección de VPN según necesidades: La elección dependerá del balance entre privacidad y funcionalidad. Mullvad e iVPN son excelentes para anonimato puro (con pagos anónimos y transparencia). ProtonVPN y AirVPN ofrecen buenos balances para el usuario general: alta seguridad, soporte amplio y velocidad estable. Cryptostorm se orienta a quienes necesitan resistencia máxima (por ejemplo, periodistas en regiones hostiles). En todo caso, conviene considerar la jurisdicción legal (suiza o europea son robustas en privacidad), la cantidad de servidores (para evitar saturación), la facilidad de uso en móviles y cualquier servicio extra (como bloqueadores de malware o modo *kill-switch* que corta la conexión si el VPN falla).

2.3 Configuración Segura de Permisos en Android

Cada aplicación en Android solicita permisos para acceder a funciones o datos sensibles (cámara, ubicación, contactos, etc.). Aplicar el **principio de confianza cero** significa no conceder ningún permiso sin evaluar su necesidad real. Debe imperar el criterio de **mínimo privilegio**: otorgar solo aquellos permisos imprescindibles para la función de la app. Esto minimiza la superficie de ataque que una aplicación maliciosa podría explotar.

- **Gestión de permisos:** Android agrupa los permisos en categorías (ubicación, cámara, micrófono, etc.). Desde Android 6.0, las apps piden permisos en tiempo de ejecución: el usuario puede permitir o denegar cada permiso por separado. Se recomienda permitir, por ejemplo, acceso a la ubicación solo mientras una app la esté usando, y denegarla en caso contrario. Revisar periódicamente los permisos concedidos permite detectar apps con solicitudes excesivas. Si una aplicación de linterna pide permisos de contactos o micrófono sin justificación, es mejor revocar esos

permisos inmediatamente. Aplicaciones desconocidas o poco confiables no deberían recibir acceso a datos privados.

- **Menor privilegio posible:** Cuantos menos permisos tenga una app, menor será su superficie de ataque. Cada permiso abre un vector adicional: con permiso de micrófono una app podría grabar audio, con permiso de ubicación podría seguir movimientos. Por eso, al instalar apps se debe revisar qué pide exactamente. En Android moderno existen opciones avanzadas: por ejemplo, se puede permitir acceso a ubicación solo "una vez", obligando a la app a pedir permiso cada vez que lo requiere. Desactivar permisos delicados (contactos, SMS, cámara) para apps que no los necesitan evita abusos. También es útil usar las opciones del sistema que limitan permisos especiales, como denegar a aplicaciones el permiso de modificación de ajustes del sistema.
- **Reducción de superficie:** Deshabilitar o desinstalar apps innecesarias reduce la exposición total. Si no se necesita NFC o Bluetooth, se pueden apagar en el dispositivo. No otorgar privilegios de root (administrador) previene que aplicaciones maliciosas comprometan el sistema completo. En la configuración de cada app, además de los permisos básicos, es posible revisar permisos "especiales" (como modificar el sistema, instalar paquetes o superponer ventanas) y deshabilitarlos para las apps convencionales. Cada permiso extra que se niegue es un posible ataque evitado.
- **Mitigación automática de riesgos:** Android incluye medidas para limitar riesgos por defecto. Por ejemplo, si una app no se usa durante mucho tiempo, el sistema puede *revocar automáticamente* sus permisos, obligando a que la aplicación vuelva a pedir acceso si se abre de nuevo. También existen controles internos que restringen ciertas acciones sospechosas (como bloquear intentos de instalar apps sin confirmación). Algunas ROMs enfocadas en seguridad (como GrapheneOS o ciertas configuraciones de LineageOS) añaden opciones avanzadas: limitación del acceso a sensores, controles de privacidad adicionales y entornos aislados para aplicaciones. Estas funciones reducen el impacto de una app maliciosa sin intervención manual.
- **Mejores prácticas:** Además de la configuración interna, conviene no instalar apps de fuentes desconocidas (fuera de tiendas oficiales). Las tiendas oficiales como Google Play disponen de filtros (Play Protect) que detectan malware conocido. Es útil también revisar qué servidores contacta cada aplicación (por ejemplo, mediante ajustes de red) y cerrar permisos de red para apps sospechosas. En resumen, una política activa de revisión y restricción de permisos, junto con actualizaciones regulares del

sistema, es clave para proteger el dispositivo contra abusos de apps maliciosas.

Sección III: Ubicación, DNS y Navegación

3.1 Amenazas de Servicios de Ubicación y Geolocalización

Los dispositivos móviles ofrecen servicios de ubicación basados en GPS, WiFi y redes celulares. Aunque útiles, pueden vulnerar la privacidad si no se gestionan adecuadamente.

- **Búsqueda de dispositivos cercanos:** Muchas aplicaciones y el propio sistema operativo buscan redes WiFi o dispositivos Bluetooth cercanos, aun sin conexión activa. Por ejemplo, un teléfono puede enviar sondas WiFi para detectar puntos conocidos, revelando indirectamente de dónde se ha ubicado antes. Asimismo, el Bluetooth puede identificar a otros aparatos en el entorno. Alguien con un escáner apropiado podría detectar estas señales (direcciones MAC o nombres de red) y deducir quién está cerca o participando en el mismo evento. Esto facilita el rastreo físico de usuarios en espacios públicos o vigilados.
- **Rastreo mediante WiFi y red celular:** Aun con el GPS apagado, las antenas WiFi y móviles aportan coordenadas de ubicación. Empresas y gobiernos usan bases de datos que asocian identificadores de routers WiFi y torres de celular con ubicaciones geográficas. Cuando el teléfono se conecta (o simplemente escanea) esas redes, revela indirectamente su posición. La red celular triangula señales a torres cercanas, calculando una ubicación aproximada del usuario. Esto significa que operadoras y terceros pueden seguir a un dispositivo usando la información de celdas y puntos de acceso cercanos. Cada conexión a Internet mediante datos móviles registra un conjunto de torres, lo que construye un rastro de movimiento.
- **Vulnerabilidades del GPS:** El GPS depende de señales satelitales. Un atacante con equipamiento especializado puede hacer *spoofing*: emitir señales falsas que engañen al receptor GPS del teléfono, haciendo que marque una ubicación errónea. También se usa *jamming* (bloqueo de señal) para inutilizar el servicio GPS en un área. Aunque estos ataques requieren hardware específico, se han reportado casos (por ejemplo, en regiones militares o en espacios públicos congestionados) donde los dispositivos dejaron de ubicarse correctamente. A nivel de usuario normal, estas amenazas son menos comunes, pero vale la pena saber que el GPS

puede ser manipulado. De momento, un teléfono no avisa si recibe señal GPS inválida, por lo que el usuario seguiría viendo ubicaciones falsas.

- **Estrategias de protección:** Para salvaguardar la privacidad, se recomienda apagar la ubicación cuando no sea necesaria. El modo avión es la medida más drástica (corta todas las radios: celular, WiFi, GPS y Bluetooth), aunque es incómodo para uso prolongado. En cambio, simplemente desactivar los servicios de ubicación y desconectar WiFi/Bluetooth cuando no se usan reduce mucho el rastreo. En Android existe la opción de desactivar la ubicación globalmente y permitirla solo a apps confiables cuando están en primer plano. También hay aplicaciones de privacidad que fuerzan la aleatorización de la dirección MAC en cada red, evitando ser rastreado por identificador. Es útil revisar los permisos de ubicación de cada app: si una aplicación no necesita GPS (p. ej. una calculadora), revocar su acceso evita que recolecte datos. En ámbitos de mayor riesgo (viajes a zonas inseguras, protestas), un teléfono dedicado con sistemas operativos de alta privacidad (ej. GrapheneOS) y sin la SIM de usuario puede minimizar fugas de ubicación.

3.2 Servicios DNS Seguros

El DNS tradicional transmite consultas en texto claro, lo que permite a cualquier observador (ISP o atacante) ver y modificar las búsquedas de dominios. Los siguientes protocolos cifran estas consultas, reforzando la privacidad:

- **DNS sobre TLS (DoT):** Encapsula las consultas DNS dentro de una capa TLS en el puerto 853. Proveedores como Cloudflare (1.1.1.1), Google (8.8.8.8) o Quad9 (9.9.9.9) ofrecen servicios DNS con DoT. A partir de Android 9 es posible configurar un “DNS privado” en los ajustes de red, habilitando DoT a nivel del sistema sin apps adicionales. Con DoT activo, la resolución de nombres se realiza cifrada de extremo a extremo al servidor DNS elegido, impidiendo que intermediarios en la red (incluido el ISP) vean qué dominios se consultan. Esto protege contra manipulación de DNS y rastreo pasivo.
- **DNS sobre HTTPS (DoH):** Similar a DoT, pero las consultas se envían dentro de peticiones HTTPS (generalmente puerto 443). Navegadores modernos (Firefox, Chrome) pueden usar DoH con proveedores como Cloudflare o NextDNS, mezclando el tráfico DNS con el resto del tráfico web cifrado. En Android existen aplicaciones (Intra, Nebulo) o servicios VPN/DNS que soportan DoH. Al usar DoH, incluso técnicas de filtrado de DNS (bloqueo regional) resultan más difíciles, pues las peticiones parecen

tráfico HTTPS normal. Sin embargo, es necesario confiar en el proveedor de DoH elegido, que verá las consultas.

- **DNSCrypt:** Protocolo más antiguo que cifra las consultas DNS usando criptografía (normalmente con curvas elípticas). Algunos servidores públicos (Quad9, OpenNIC, Cloudflare) lo soportan. Funciona con un cliente especial en el dispositivo que encripta la consulta DNS antes de enviarla. Aunque hoy DoT y DoH son más comunes, DNSCrypt sigue siendo una alternativa válida para quienes ya lo soportan. Ofrece protección similar: nadie en medio puede leer ni manipular las peticiones DNS.
- **Comparativa y configuración:** Tanto DoT como DoH protegen las consultas DNS, pero difieren en la implementación. DoT normalmente se activa a nivel de sistema operativo (lo usa cualquier aplicación). DoH puede activarse por aplicación (como en un navegador) o mediante apps específicas. Para configurarlos, en Android se puede usar la opción "Privado" en la configuración de WiFi o apps que permitan establecer un DNS seguro. En ambos casos, elegir un servidor confiable (que tenga política de no registro) es fundamental. DoH por HTTPS puede pasar inadvertido en redes restringidas, mientras que DoT estándar es fácil de configurar a nivel de sistema. En general, usar cualquier forma de DNS cifrado mejora la privacidad en comparación con el DNS en texto claro.
- **Beneficios adicionales:** Además de privacidad, algunos servidores DNS seguros agregan filtros opcionales (malware, phishing o trackers). Por ejemplo, Quad9 bloquea automáticamente dominios maliciosos conocidos, y NextDNS permite configurar listas de bloqueo personalizadas (publicidad, adult content, etc.). Esto añade seguridad adicional sin instalar antivirus. Sin embargo, se debe usar con cuidado: los filtros podrían negar acceso a sitios legítimos si son clasificados erróneamente. En conjunto, los DNS cifrados, junto con VPNs y conexiones HTTPS, completan una estrategia de defensa de la privacidad en navegación y acceso a recursos en línea.

3.3 Amenazas en Navegación Web

La navegación web expone a los usuarios a múltiples técnicas de rastreo y recolección de datos. Comprenderlas y mitigarlas es esencial para la privacidad.

- **Cookies de seguimiento:** Sitios y redes publicitarias almacenan cookies en el navegador para reconocer al usuario entre visitas. Las *cookies de terceros* (colocadas por anuncios o scripts externos) siguen al usuario en diferentes páginas web, creando un perfil de intereses. Incluso si se borran

las cookies locales, los rastreadores pueden restablecer cookies persistentes o usar otros mecanismos de almacenamiento (por ejemplo, **localStorage**) para mantener los identificadores. Estas técnicas operan a menudo sin el consentimiento informado del usuario, por lo que es difícil escapar de ellas con navegación normal.

- **Rastreadores y scripts:** Muchos sitios incluyen scripts de terceros (Google Analytics, píxeles de seguimiento, botones sociales) que monitorizan la actividad. Estos scripts recopilan datos de navegación y los envían a servidores externos. De este modo, grandes corporaciones publicitarias pueden construir un historial completo de un usuario en la web, aun sin que este interactúe directamente con sus anuncios. Por ejemplo, hay *web beacons* (imágenes invisibles), *fingerprintings* (medición del navegador), y rastreadores que cargan contenido desde dominios de seguimiento en cada página. En conjunto, esta red de scripts permite perfilar movimientos, hábitos de compra e incluso inferir datos personales delicados.
- **Publicidad dirigida y perfilado:** Los datos recolectados alimentan los algoritmos de publicidad. Basado en el perfil, los anunciantes muestran anuncios segmentados. Por ejemplo, visitar repetidamente sitios de deportes hará que aparezcan anuncios de equipamiento deportivo. Este perfilado no solo invade la privacidad: puede asociar la navegación con información sensible (opiniones políticas, creencias religiosas, salud, etc.) sin consentimiento. Cada interacción en la web se convierte en una señal para definir al usuario. Los resultados se combinan con datos demográficos o comportamentales para construir un perfil digital muy preciso. Los anunciantes también comercian con estos datos; un tercero podría comprar información de perfiles agregados y cruzarla con otros datos públicos.
- **Fingerprinting de dispositivos:** Más allá de las cookies, el *fingerprinting* de navegador consiste en recopilar características del dispositivo para crear una huella única. Esto incluye elementos como: agente de usuario, zona horaria, lista de fuentes instaladas, datos del canvas gráfico, aceleración WebGL, plugins instalados, entre otros. Combinando varios atributos, es posible identificar a un usuario en sucesivas visitas incluso después de borrar cookies. El fingerprinting es difícil de bloquear completamente porque no depende de almacenar datos en el dispositivo, sino de observar su configuración. Con técnicas avanzadas, empresas pueden reconocer hasta el mismo dispositivo web navegando en modo incógnito, ya que la “huella” persiste a nivel de hardware y configuración.

- **Estrategias de bloqueo y privacidad:** Para contrarrestar estas amenazas se recomiendan navegadores y herramientas enfocadas en privacidad. Extensiones como *uBlock Origin* o *Privacy Badger* bloquean anuncios y rastreadores conocidos, impidiendo que los scripts externos se carguen. Navegar en modo privado o incógnito limita la cantidad de datos persistentes: no guarda historial de navegación ni cookies permanentes al cerrar la sesión. Además, existen extensiones anti-fingerprinting (NoScript, CanvasBlocker) que neutralizan o modifican los datos que facilitan la identificación, como deshabilitar JavaScript o aleatorizar la información que envía el navegador. Opciones como Tor Browser llevan esto más lejos: aíslan cada pestaña en una sesión distinta, borran cookies automáticamente y llevan protecciones integradas contra el fingerprinting. En conjunto, combinar VPN con navegadores seguros y bloqueadores reduce drásticamente las posibilidades de ser rastreado en línea.

Sección IV: Defensa en Profundidad

4.1 Criptodivisas y Privacidad Financiera

Las criptomonedas permiten transacciones en redes distribuidas, pero su pseudonimato puede no garantizar anonimato completo. Es clave manejar correctamente las carteras y elegir criptomonedas enfocadas en privacidad.

- **Blockchain y anonimato:** Las transacciones quedan registradas en una cadena de bloques pública, accesible para todos. Cada operación incluye las direcciones de envío y recepción y el monto. Si bien no aparece el nombre real de los participantes, la transparencia permite analizar patrones. Por ejemplo, si un usuario publica su dirección, cualquiera puede seguir sus transacciones. Incluso sin identificar nombres, firmar una transacción con una dirección reutilizada puede vincular todas esas transacciones entre sí. En la práctica, el anonimato depende de mantener las direcciones fuera del dominio público o mezclar las monedas.
- **Carteras (wallets) y gestión de claves:** Las criptomonedas se guardan en *wallets*, que gestionan pares de claves criptográficas. Para mayor privacidad, se recomienda usar *wallets HD* (determinísticas jerárquicas) que generan una dirección nueva para cada transacción, dificultando vincular todas las operaciones a un mismo usuario. Las claves privadas deben almacenarse con extremo cuidado: una hardware wallet (como Trezor o Ledger) proporciona aislamiento físico, evitando que malware en el móvil o PC las robe. También es buena práctica cifrar copias de

seguridad de las claves y no guardar las llaves privadas en línea. Es importante separar las criptomonedas de uso diario de las de ahorro: mantener fondos a largo plazo en carteras frías desconectadas de la red mejora la seguridad.

- **Monedas de privacidad:** Algunas criptomonedas están diseñadas para ofuscar el origen y destino de los fondos de forma nativa. Monero (XMR) utiliza firmas de anillo y direcciones ocultas (stealth addresses), mezclando cada transacción con otras para ocultar quién envía y quién recibe. Zcash (ZEC) permite transacciones protegidas basadas en pruebas de conocimiento cero (zk-SNARKs), ocultando montos y participantes. Estas monedas protegen la privacidad de forma más fuerte que Bitcoin, que es solo pseudónimo. No obstante, su uso requiere carteras compatibles y, en algunos casos, esperar tiempos de confirmación mayores debido a los procesos criptográficos adicionales.
- **Protección de datos financieros:** Además de la criptografía integrada, la seguridad personal es clave. Es recomendable no vincular cuentas de intercambio centralizado (exchanges) que requieran KYC con las direcciones personales de criptos. Cada transacción debería pasar por una cartera de privacidad o mezclador para romper trazas directas. No publicar direcciones en foros o redes sociales evita que terceros asocien transacciones con una persona. Separar billeteras para distintos fines (por ejemplo, otra para donaciones públicas) limita el impacto en caso de filtración. Cifrar backups de las carteras y almacenarlos en medios offline (como papel con cifrado o hardware dedicado) previene pérdidas. En definitiva, el uso de herramientas de cifrado y buenas prácticas de gestión de claves asegura que la privacidad financiera se mantenga lo más alta posible.

4.2 Criptografía para Seguridad de Información

La criptografía es la base de la seguridad de la información en dispositivos móviles. Aplicar cifrado adecuado a datos y comunicaciones garantiza confidencialidad, integridad y autenticidad.

- **Cifrado de dispositivos:** Muchos teléfonos ofrecen cifrado completo del almacenamiento. Al activarlo (mediante PIN o contraseña fuerte), todos los archivos internos se cifran con AES (generalmente de 128 o 256 bits). Esto significa que si el dispositivo se pierde o es robado, un atacante no puede leer el contenido sin la clave. Android e iOS implementan esto de forma transparente: el disco de datos se encripta usando claves derivadas de la

contraseña del usuario. Es fundamental elegir un PIN/contraseña largo (por ejemplo, un PIN de 6+ dígitos o contraseña alfanumérica) para asegurar que la clave de cifrado sea difícil de adivinar. Sin un cifrado activo, cualquier persona con acceso físico podría extraer datos sensibles.

- **Cifrado de archivos y datos:** Más allá del cifrado total del dispositivo, es útil cifrar archivos individuales o carpetas de alta sensibilidad (fotos, documentos, notas). Herramientas como GPG (para correo o textos) o soluciones de contenedores cifrados (VeraCrypt) permiten proteger archivos con contraseñas separadas. En Android existen apps que cifran carpetas o que almacenan archivos de forma cifrada. El cifrado simétrico (AES-256) se recomienda para datos en reposo, usualmente con modos seguros como XTS. Por ejemplo, antes de compartir un archivo por correo o nube, cifrarlo con una contraseña resistente previene que intermediarios o proveedores de nube lo lean sin permiso. Esto es especialmente útil para respaldos o información altamente confidencial.
- **Cifrado de conexiones:** Para proteger la comunicación en redes, los protocolos TLS (SSL) cifran la mayoría del tráfico de Internet (HTTPS para web, SMTPS/IMAPS para correo, etc.). Usar siempre HTTPS en sitios web evita que alguien intercepte los datos entre el móvil y el servidor. Las aplicaciones móviles de mensajería segura (Signal, WhatsApp) utilizan protocolos de cifrado extremo a extremo (Signal Protocol) que aseguran que solo el emisor y receptor legítimos puedan leer los mensajes. También es recomendable usar VPNs cifradas (por ejemplo, OpenVPN o WireGuard) para asegurar el tráfico general del dispositivo. En redes abiertas, esto impide que intrusos leean correos, chats o contraseñas que viajan por WiFi pública.
- **Algoritmos y aplicación:** Es importante usar algoritmos estándar de la industria. Para cifrado simétrico se prefiere AES (idealmente AES-256) con modos autenticados (AES-GCM o ChaCha20-Poly1305). Para cifrado asimétrico, RSA con claves de al menos 3072 bits o algoritmos de curva elíptica como ECC (Curve25519) son recomendados. Para funciones de hash, SHA-256 o SHA-3 son seguros. Por ejemplo, al generar un par de llaves PGP para correo, es común usar RSA-4096 para la clave de firma y AES-256 para cifrar mensajes. Herramientas criptográficas en el móvil (mensajería cifrada, navegadores HTTPS, almacenamiento cifrado) deben implementarse preferentemente con bibliotecas probadas y configuraciones seguras, evitando algoritmos obsoletos (como DES, RC4 o MD5) que ya han sido quebrantados.

- **Herramientas prácticas:** Para el usuario común existen soluciones accesibles. Aplicaciones de mensajería con cifrado fuerte (Signal, Telegram en modo secreto) protegen el contenido de chats. Navegadores con HTTPS estricto y extensiones que fuerzan conexiones seguras evitan ataques de intermediario. Almacenamiento en la nube cifrado cliente-lado (Cryptomator, Tresorit) asegura que la empresa proveedora no pueda leer archivos. También hay apps de cifrado de contraseñas (Bitwarden, KeePass) y gestores de archivos cifrados. En suma, cada capa de comunicación y almacenamiento en el móvil debería estar cifrada: disco completo, archivos sensibles y conexiones de red, utilizando algoritmos sólidos para impedir accesos no autorizados.

4.3 Darknets y Anonimato en Comunicaciones

Las **redes oscuras** (darknets) son arquitecturas de comunicación superpuestas a Internet, diseñadas para maximizar el anonimato y la resistencia a la censura. Entre las más conocidas están Tor, I2P y Freenet. No son ilegales en sí mismas; su uso legítimo incluye proteger informantes, periodistas o usuarios en entornos represivos.

- **Tor:** (The Onion Router) enruta el tráfico de Internet a través de múltiples nodos voluntarios para ocultar su origen. El cliente Tor (Tor Browser, por ejemplo) cifra los datos del usuario en capas sucesivas de cifrado (como una cebolla). Cada nodo del circuito desencripta una capa: primero el de entrada ve la IP del usuario pero no el destino; el nodo intermedio reenvía los datos sin conocer la fuente ni el destino final; el nodo de salida descifra la capa final y envía la petición al servidor de destino. En conjunto, ningún punto conoce por completo el trayecto. Tor Browser permite además acceder a sitios normales de manera anónima y a "**servicios ocultos**" (.onion), donde tanto el cliente como el servidor permanecen ocultos. Los sitios .onion garantizan que ni el proveedor de contenido conozca la IP del visitante, ni viceversa. Esto es clave para evadir censuras geográficas y proteger identidades.
- **I2P:** (Invisible Internet Project) es una darknet peer-to-peer. Utiliza un enrutamiento tipo cebolla llamado *garlic routing* (mensaje empaquetado en múltiples capas) para ofuscar la ruta. A diferencia de Tor, I2P está diseñada más para servicios internos. Los sitios web en I2P (llamados *eepsites*) son accesibles solo dentro de la red I2P. Cada usuario de I2P actúa como cliente y router a la vez, reenviando tráfico para otros. La comunicación en I2P está cifrada de extremo a extremo entre pares. Se usa

principalmente para mensajería anónima, foros internos y hospedaje de contenido bajo demanda sin revelar IPs. Al carecer de nodos de salida hacia Internet pública, no hay puntos que puedan observar el tráfico saliente; todo permanece cifrado dentro de la red.

- **Freenet:** Es una red descentralizada de almacenamiento anónimo. Los usuarios comparten espacio en disco para el almacenamiento comunitario. Cuando alguien inserta datos (archivos, sitios), estos se reparten cifrados en varios nodos basándose en el hash de su nombre. Para recuperar información, la búsqueda se propaga por la red y los datos se reconstruyen de varios nodos. En Freenet no hay comunicación directa de persona a persona; solo datos cifrados. Esto significa que ni el origen ni el destino pueden rastrearse. Freenet está optimizado para publicar contenido de forma resistente: si uno o varios nodos desaparecen, otros mantienen copias. Toda la comunicación en Freenet se cifra de extremo a extremo, protegiendo la fuente y el contenido a nivel global.
- **Nodos y pares en redes descentralizadas:** En Tor se distinguen tres tipos de nodos: *entry guard* (conoce la IP del usuario pero no el destino final), *relay medio* (reenvía datos sin saber origen completo) y *exit node* (último salto que desencripta la capa final y accede al recurso de Internet; puede ver el tráfico saliente en texto claro si no está cifrado). En I2P y Freenet no hay nodos de salida al Internet tradicional: las conexiones ocurren dentro de la propia red oculta. En todas estas redes, cada nodo voluntario contribuye recursos (ancho de banda, almacenamiento) para el bien común. Una desventaja potencial es que un nodo comprometido o malintencionado podría intentar correlacionar tráfico: por ejemplo, en Tor el nodo de salida ve el destino, y si alguien controla el nodo de entrada y salida simultáneamente podrían intentar descubrir al usuario. Sin embargo, las capas de cifrado y la rotación frecuente de rutas dificultan mucho estos ataques.
- **Anonimato y resistencia a la censura:** Estas redes están pensadas para que ni gobiernos ni proveedores de Internet puedan rastrear fácilmente la actividad de los usuarios. Por ejemplo, usar Tor o I2P permite acceder a servicios bloqueados o censurados en algunos países, ya que el acceso se hace a través de un túnel cifrado. Periodistas y activistas en países represivos las usan para comunicarse sin revelar su ubicación. El anonimato garantiza que ni el contenido ni las identidades se revelen. Sin embargo, no es infalible: análisis de tráfico avanzados o errores del usuario (divulgar información personal dentro de la red) pueden comprometer el anonimato. Por ello es crucial combinar estas redes con precauciones

adicionales, como no usar identificadores reales, cambiar hábitos de navegación y, cuando sea posible, redondear el anonimato con otras herramientas (por ejemplo, navegadores seguros, sistemas operativos live como Tails).

- **Comunicación segura en darknets:** Para participar se utilizan clientes especializados: Tor Browser para Tor (.onion), clientes específicos de I2P (.i2p) o software de Freenet. Dentro de estas redes, todas las comunicaciones se cifran por defecto: los mensajes, correos anónimos y sitios sólo son legibles por quienes conocen la clave. Por ejemplo, mensajeros internos de I2P cifran todo el contenido con criptografía fuerte y ocultan metadatos. Es fundamental usar estas redes respetando las reglas de anonimato: no revelar información personal ni direcciones de correo tradicionales. Conjuntar redes anónimas (usando VPN o Tor) y comunicaciones cifradas de extremo a extremo (como chats en Signal o correos PGP incluso dentro de la red) fortalece aún más la defensa. En esencia, las darknets aportan capas extra de privacidad y permiten la autodefensa electrónica en comunicaciones cuando la libertad de expresión o la seguridad personal están amenazadas.

La soberanía digital se revela como un imperativo ineludible en un entorno donde la vigilancia ubicua y el control de los datos erosionan libertades fundamentales, exigiendo una respuesta que trascienda la mera acumulación de herramientas técnicas para convertirse en una postura existencial de resistencia activa y responsabilidad compartida. El análisis de amenazas —desde redes WiFi vulnerables y Bluetooth inseguro hasta rastreo por geolocalización, fingerprinting y perfiles comportamentales— demuestra que ningún vector aislado es letal, pero su combinación configura un entramado opresivo que solo puede contrarrestarse mediante una estrategia de defensa en profundidad: contraseñas de alta entropía, gestores de claves, VPNs con políticas rigurosas de no registro, DNS cifrado, actualizaciones constantes, permisos mínimos en aplicaciones, cifrado de almacenamiento y comunicaciones, y el uso ponderado de redes oscuras como Tor o I2P para escenarios de alto riesgo. Cada capa aporta resiliencia, pero el eslabón más frágil sigue siendo el factor humano, por lo que la educación continua y la conciencia situacional resultan tan cruciales como los algoritmos más robustos; la reutilización de credenciales, la conexión a redes fraudulentas o la instalación de apps maliciosas pueden anular cualquier protección técnica en segundos. Más allá de lo individual, esta problemática adquiere una dimensión política ineludible: el control de los datos personales

constituye una nueva forma de poder que amenaza la democracia, y herramientas como Monero, Zcash, Tor o el cifrado de extremo a extremo no son meros gadgets, sino instrumentos de empoderamiento ciudadano que permiten resistir la vigilancia masiva y preservar espacios de autonomía. La evolución constante de las amenazas y las defensas descarta la seguridad absoluta, pero impone una gestión inteligente del riesgo que equilibre protección y usabilidad según el perfil de cada usuario. En definitiva, la autodefensa electrónica no es un lujo técnico, sino una práctica cotidiana de ciudadanía activa que exige decisiones informadas, solidaridad entre vulnerables, exigencia de marcos legales protectores y una revalorización cultural de la privacidad como bien común; solo así podremos construir barreras efectivas que salvaguarden nuestra dignidad y autonomía en la era digital, afrontando este desafío con la seriedad y el compromiso que merece.